REMARKS

The Examiner is thanked for the performance of a thorough search.

No claims have been added, canceled, or amended. Hence, Claims 1, 4-21, 23-25, 27-29, 31-32, 34-37, 39-42, and 44-47 are pending in the present application.

Each issue raised in the Office Action mailed September 2, 2008 is addressed hereinafter.

I. REJECTIONS UNDER 35 U.S.C. § 112, FIRST PARAGRAPH

Claims 1, 21, 25, and 29 were rejected under 35 U.S.C. § 112, first paragraph as allegedly failing to comply with the written description requirement. This rejection is respectfully traversed.

First, the Office Action asserts that the specification as originally filed and the original claims did not describe "security information defining a number of required signatures and required principals." This assertion is incorrect.

Each of original Claims 3, 4, 13, and 14 includes the feature of:

> receiving, in association with a particular configuration directive, security information **defining a number of** required signatures and required principals. (Emphasis added.)

Further, when this feature of original Claims 3, 4, 13, and 14 is considered in light of the specification (e.g., in light of paragraphs [0032], [0044], [0059]-[0061], [0069], [0071]), this feature would clearly and more than reasonably convey to one of ordinary skill in the art that the Applicant had possession of the subject matter in this feature at the time the present application was filed. Specifically, one of ordinary skill in the art would clearly consider that at the time of filing the Applicant had possession of and described in the specification "security information defining a number of required signatures and required principals" that is associated with a particular configuration directive.

Second, the Office Action asserts that the specification as originally filed and the original claims did not include the term "collective authority." This assertion is incorrect.

Each of original Claims 2 and 12 includes the feature of:

> verifying that the one or more digital signatures is valid and that one or more principals respectively associated with the digital signatures have **collective authority** to perform the directives on the host. (Emphasis added.)

Thus, the Office Action is not correct in asserting that the original specification and the original claims did not disclose the term "collective authority." Further, when the above feature of original Claims 2 and 12 is considered in light of the specification (e.g., in light of paragraphs [0030], [0059]-[0061], [0074]), this feature would clearly and more than reasonably convey to one of ordinary skill in the art that the Applicant had possession of and described the term "collective authority" as well as embodiments in which verification is performed of whether multiple principals have "collective authority" in order to apply configuration directive(s) on a host.

For the foregoing reasons, reconsideration and withdrawal of the rejections of Claims 1, 21, 25, and 29 under 35 U.S.C. § 112, first paragraph is respectfully requested.

II. ISSUES RELATING TO THE CITED ART

A. INDEPENDENT CLAIM 1

Claim 1 was rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over Bosler, U.S. Patent Application Publication No. US 2005/0010757 ("BOSLER") in view of Kinnis et al., U.S. Patent No. 6,959,382 ("KINNIS"). The rejection is respectfully traversed.

Among other features, Claim 1 comprises the features of:

> **receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;**
> ... ;
> **verifying** that the two or more digital signatures are valid and **that two or more principals respectively associated with the two or more digital signatures**

have collective authority to perform the configuration directives on the host network element;

applying the configuration directives to the host network element only when the two or more digital signatures are verified successfully;

wherein applying the configuration directives comprises **applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals**.

It is respectfully submitted that BOSLER and KINNIS do not describe or suggest the features of Claim 1 that are highlighted above.

The Office Action asserts that in paragraphs [0058] and [0069] BOSLER describes the features of Claim 1 of: receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals; and applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals. The Office Action also asserts that the present application: (1) does not disclose security information defining a number of required signatures by the required principals (Office Action, pp. 2-3, numbered paragraph 3.1); and (2) does not disclose applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals (Office Action, pp. 4-5, numbered paragraph 3.4). These assertions are incorrect.

As discussed above with respect to the rejection under 35 U.S.C. § 112, first paragraph, the original Claims 3, 4, 13, and 14 include the feature of receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals. Further, the original Claims 3, 4, 13, and 14 also include the feature of applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals. Thus, contrary to the assertions in the Office Action, the present application clearly describes that a number of required signatures and required principals may be associated with a particular configuration directive and that a

particular configuration directive is to be applied on a host only when a received configuration information has the number of required signatures by the required principals.

Further, in paragraph [0058], BOSLER describes that a first node and a second node may establish a secure session by exchanging a management message that may be authenticated by a digital signature. Specifically, BOSLER describes that the first node and the second node may establish a secure session by mutual authentication using their respective public keys. (Paragraph [0058], lines 9-12.) The first node may send a management message to the second node (paragraph [0058], lines 7-9), where the management message may be signed by a digital signature generated by using the first node's private key (paragraph [0058], lines 13-17). The second node verifies the authenticity of the first node based on the public key of the first node, where verifying the authenticity of the first node includes verifying the authenticity of the first node's public key by a certificate of this public key. (See paragraph [0058], lines 19-28.) In paragraph [0069], BOSLER describes a management server that receives information from distributed agents on the nodes being managed, and that sends management requests to the agents.

Significantly, however, neither paragraphs [0058] and [0069] nor any other paragraph of BOSLER describes or suggests that a management message includes a number of required signatures and required principals, where the number may be used in determining whether to apply a configuration command. Moreover, while in paragraph [0069] BOSLER may be describing that a management server may be capable of sending management requests to the nodes being managed, BOSLER does not describe that the management server checks or otherwise determines anything about a number of required signatures and required principals that are associated with a management request. In fact, it appears that paragraphs [0058] and [0069] of BOSLER refer to two completely different and separate embodiments – the embodiment in

paragraph [0058] refers to establishing secure sessions between nodes by exchanging a management message, while the embodiment in paragraph [0069] refers to a management server that sends management requests to nodes that are being managed.

In contrast, Claim 1 comprises the features of receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals; and applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals. According to these features of Claim 1, a particular configuration directive is applied only when the configuration information (which includes the particular configuration directive) has the number of required signatures and principals, which number is specified in previously received security information.

The Office Action asserts that in col. 3, lines 3-28, col. 4, lines 25-34, and col. 10, lines 38-67, KINNIS describes the feature of Claim 1 of verifying that the two or more digital signatures are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the configuration directives on the host network element. The Office Action also asserts that the present application does not disclose this feature of Claim 1. (See Office Action, p. 3, numbered paragraph 3.2, and pp. 3-4, numbered paragraph 3.3) These assertions are incorrect.

As discussed above with respect to the rejection under 35 U.S.C. § 112, first paragraph, when the original Claims 2 and 12 are considered in light of the specification (e.g., in light of paragraphs [0030], [0059]-[0061], [0074]), the features in these claims would clearly and more than reasonably convey to one of ordinary skill in the art that the Applicant had possession of and described the term "collective authority" as well as embodiments in which verification is performed of whether multiple principals have "collective authority" in order to apply

configuration directive(s) on a host. Thus, contrary to the assertions in the Office Action, the present application clearly describes the feature of Claim 1 of verifying that the two or more digital signatures are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the configuration directives on the host network element.

Further, in col. 3, lines 3-24, KINNIS describes a digital signature service that can be used by multiple users to sign a single document. A first user invokes the digital signature service to generate a first signature file corresponding to the document. After receiving the first signature file, a second user (e.g., a party to a contract with the first user) verifies through the digital signature service that the content of document is not altered and authenticates the first user as the user who digitally signed the document. Then, if the second user wishes to digitally sign the document, the second user may invoke the digital signature service to generate a second signature file for the document. In col. 10, lines 38-67, KINNIS further describes that a third user may also wish to become signatory to the document. The third user invokes the digital signature service to verify the contents of the document and to verify the authenticity of the second user and of the first user. If the third user then wishes to become a signatory to the document, the third user invokes the digital signature service to sign the document that was signed by the second user. In col. 4, lines 25-34 KINNIS describes that a document may be a file, a message, or content of any type that a user wishes to digitally sign.

Significantly, however, KINNIS does not describe or suggest anything about verifying whether the two or three users have **collective authority** to perform any configuration directives on a network element, as featured in Claim 1. While KINNIS may be describing that two or three users may digitally sign the same document separately from each other, KINNIS does not describe or suggest that the two or three users have any collective authority that they can convey

by singing the same document. Rather, KINNIS describes that any user who wishes to digitally sign the document may do so by using the digital signature service. (See, for example, KINNIS col. 10, lines 27-29, 41-45, 53-54, and 60-64.) In other words, KINNIS describes that each user may have authority to sign a document separately and independently from any other user. Further, while the users in KINNIS may digitally sign document with digital signatures, KINNIS does not describe that these digital signatures are used in any way to determine whether the users have some authority to perform any action, such as applying configuration directives as featured in Claim 1. Rather, the users in KINNIs digitally sign the document in order to verify the integrity of the document and the authenticity of the user signing the document. (See, for example, KINNIS, col. 2, lines 32-36.)

In contrast, Claim 1 comprises the feature of verifying that the two or more digital signatures are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the configuration directives on the network element. It is respectfully submitted that verifying the integrity of a document and authenticating the users that digitally signed the document (as described in KINNIS) is not equivalent to verifying that two or more principals have collective authority to perform configuration directives on a network element (as featured in Claim 1).

Finally, the Applicant previously argued that there is no rational reason or other evidentiary underpinning for modifying the BOSLER system to use multiple digital signatures as described in KINNIS, as is required to sustain an obviousness rejection under 35 U.S.C § 103(a). Specifically, the Applicants argued that since BOSLER describes using a digital signature for the purpose of authenticating a sender node, the sender node does not need to send more than one signature in order to authenticate itself with the receiving node. In fact, BOSLER does not describe or suggest that a node may be assigned more than one private key, which means that in

BOSLER a node cannot sign a management message with more than one digital signature. Thus, one of ordinary skill in the art would have absolutely no reason, need, or rationale whatsoever for modifying the BOSLER system to use multiple digital signatures as described in KINNIS.

The present Office Action, however, does not address this argument of the Applicant and does not provide a rational reason or other evidentiary underpinning about why one of skill in the art would decide to modify the BOSLER system to use multiple digital signatures as described in KINNIS, given the fact that the BOSLER system uses a digital signature for the sole purpose of authenticating a sender node.

Rather, in pp. 5-6, numbered paragraph 3.5, the Office Action asserts that there is no disclosure in KINNIS that discredits or discourages the usage of any type of combined authority. The Applicants respectfully disagree with this assertion because in numerous passages KINNIS expressly describes that any user who wishes may digitally sign a document. (See, for example, col. 3, lines 14-17, col. 4, lines 25-27, and col. 10, lines 27-29, 41-45, 53-54, and 60-64.) Since KINNIS pre-conditions the digital signing of documents on the wishes of each individual user, KINNIS clearly teaches against use of multiple digital signatures to convey a collective authority for the purpose of performing a particular action, such as applying configuration directives on a host network element as featured in Claim 1.

For the above reasons, BOSLER and KINNIS do not describe or suggest all features of Claim 1. Thus, Claim 1 is patentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS. Reconsideration and withdrawal of the rejection of Claim 1 is respectfully requested.

B. INDEPENDENT CLAIM 8

Claim 8 was rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of Sudia et al., U.S. Patent Application Publication No. US 2002/0013898 ("SUDIA"). The rejection is respectfully traversed.

Among other features, Claim 8 comprises the features of:

> receiving **configuration control information** that **includes a time period during which a valid digital signature is required for applying one or more particular configuration directives**;
> …;
> **only when the date-time value is within the time period and the one or more configuration directives have not been previously received during the time period, attempting to verify the one or more digital signatures** based on the trust information, **and applying the configuration directives** to a network element only when the one or more digital signatures are verified successfully.

The Office Action asserts that the above features of Claim 8 are described in paragraphs [0071] and [0073] of BOSLER and in paragraph [0249] of SUDIA. This assertion is incorrect.

In paragraph [0071], BOSLER states:

> The certification server 13 is arranged to receive a certificate-grant request and to issue the requested public-key certificate, provided that **the time interval between the initialization time and the request time** (i.e. the time when the certificate-grant request was received at the certification server 13) **is within a maximum time interval 14 stored**, for example, in the certification server 13. The time interval 14 is configurable by an authorized user, e.g. a network operator. In order to decide whether the certificate is granted, the certification server accesses the management information database 12 and recalls the stored initialization time for the managed node 4 from which the certificate-grant request was received. (Emphasis added.)

The time interval described in the above paragraph is an interval within which a node must request a public key certificate. Significantly, a certificate server would grant a public key certificate to a node only if the node requests the certificate within a particular time interval after a management agent is initialized/installed on the node. (See also at least BOSLER, paragraph [0010]; paragraph [0073], lines 17-22.) Thus, the time interval described by BOSLER is used to determine whether or not a node would be granted a public key certificate.

In contrast, Claim 8 includes the feature of receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives. A time period during which a valid signature is required for applying a configuration directive on a network element (as featured in Claim 8) is

completely different from a time interval used to determine whether or not a node would be granted a public key certificate (as featured in BOSLER).

Further, in paragraph [0058] BOSLER describes that a first node and a second node may establish a secure session by exchanging a management message that may be authenticated by a digital signature. However, BOSLER does not describe or suggest that a management message sent by the first node includes any time interval. In fact, there is absolutely nothing in BOSLER that describes or suggests that management messages exchanged between nodes may include any time intervals indicating that configuration operations specified in the messages can be applied on nodes only during these time intervals. In contrast, the time period featured in Claim 8 is used to determine whether verification of one or more digital signatures would be attempted and whether one or more configuration directives would be applied to a network element.

It is respectfully submitted that SUDIA fails to cure the deficiencies of BOSLER with respect to the above features of Claim 8. Specifically, in paragraph [0249] SUDIA describes that when a primary user wants to delegate signatory authority to a delegate user, the primary user issues a substitution certificate that includes a time limit. Significantly, the time limit indicates a time period during which the substitution certificate is valid.

In contrast, Claim 8 features configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives. It is respectfully submitted that a time limit during which a substitution certificate is valid (as described in SUDIA) is very different from a time period during which a valid digital signature would be required for applying one or more particular configuration directives (as featured in Claim 8).

Further, Claim 8 includes the features of: receiving configuration information comprising, among other things, one or more configuration directives and a date-time value;

determining whether the received date-time values is within the time period; determining if the one or more configuration directives have been previously received during the time period; and only when the date-time value is within the time period and the one or more configuration directives have not been previously received during the time period, attempting to verify the one or more digital signatures based on the trust information, and applying the configuration directives to a network element only when the one or more digital signatures are verified successfully. These features of Claim 8 indicate that the time period received in the configuration control information is used to prevent the application of the same one or more configuration directives more than once during that time period. In contrast, the time limit described in SUDIA is used to perform a completely different functionality, namely to limit the period of time during which a delegate user can use a substitution certificate to sign documents on behalf of the the primary user.

For the above reasons, BOSLER and SUDIA do not describe or suggest all features of Claim 8. Thus, Claim 8 is patentable under 35 U.S.C. § 103(a) over BOSLER in view of SUDIA. Reconsideration and withdrawal of the rejection of Claim 8 is respectfully requested.

C. INDEPENDENT CLAIM 18

Claim 18 was rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of SUDIA.

Claim 18 includes features similar to the features of Claim 8 discussed above. Thus, Claim 18 is patentable under 35 U.S.C. § 103(a) over BOSLER in view of SUDIA for at least the reasons given above with respect to Claim 8. Reconsideration and withdrawal of the rejection of Claim 18 is respectfully requested.

D. INDEPENDENT CLAIMS 21, 25, AND 29

Claims 21, 25, and 29 were rejected as allegedly unpatentable under 35 U.S.C. § 103(a)

over BOSLER in view of KINNIS.

Claims 21, 25, and 29 include features similar to the features of Claim 1 discussed above, except in the context of an apparatus and a computer-readable medium. Thus, Claims 21, 25, and 29 are patentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS for at least the reasons given above with respect to Claim 1. Reconsideration and withdrawal of the rejection of Claims 21, 25, and 29 is respectfully requested.

E. DEPENDENT CLAIMS 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, AND 44-47

Claims 4-7, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 were rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS. Claims 9-14 were rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of SUDIA. Claims 15-17 and 19-20 were rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of SUDIA and further in view of KINNIS.

Each of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 depends from one of independent Claims 1, 8, 18, 21, 25, and 29, and thus includes each and every feature of the independent base claim. Thus, each of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 is allowable for at least the reasons given above for Claims 1, 8, 18, 21, 25, and 29. In addition, each of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 introduces one or more additional features that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those features is not included at this time. Therefore, it is respectfully submitted that Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 are allowable for the reasons given above with respect to Claims 1, 8, 18, 21,

25, and 29. Reconsideration and withdrawal of the rejections of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 is respectfully requested.

III. CONCLUSION

The Applicants believe that all issues raised in the Office Action have been addressed. Further, for the reasons set forth above, the Applicants respectfully submit that allowance of the pending claims is appropriate. Reconsideration of the present application is respectfully requested in light of the remarks herein.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, a law firms check for the petition for extension of time fee is enclosed herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to charge any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Dated: November 25, 2008

/StoychoDDraganoff#56181/
Stoycho D. Draganoff
Reg. No. 56,181

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1080 ext. 208
Facsimile No.: (408) 414-1076